Information Assurance Division

Marine Corps Systems Command

Mr. Mike Davis, Director

http://www.marcorsyscom.usmc.mil/sites/ia

INCREASING SECURITY AWARENESS FOR THE INFORMATION WARRIOR

Information Assurance (IA)

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

INFORMATION ASSURANCE DIVISION
MARINE CORPS SYSTEMS COMMAND

Mission:

To support the implementation of Information Assurance (IA) policies and practices for the Marine Corps in its effort to develop and field systems and applications that ensure confidentiality, authentication, non-repudiation, integrity, and availability of information.

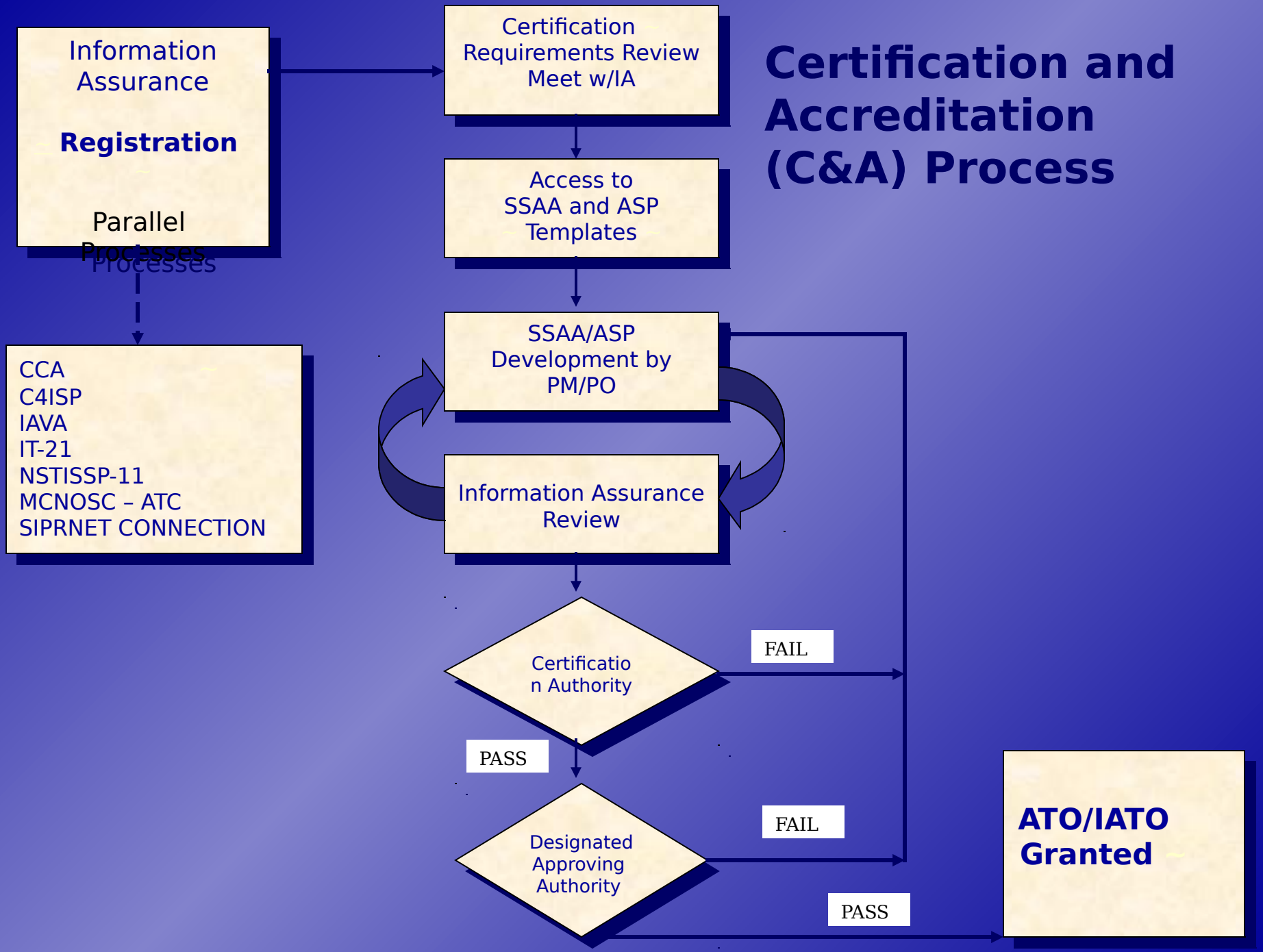
INCREASING SECURITY AWARENESS FOR THE INFORMATION WARRIOR

INFORMATION ASSURANCE DIVISION
MARINE CORPS SYSTEMS COMMAND

What does this mean to you?

- **Interfacing with the IA Team**
- **Budgeting for IA Requirements**
- **Achieving DITSCAP Certification & Accreditation**
- **Understanding the C&A Process**

Certification and Accreditation (C&A) Process



formation Assurance Web Site - Microsoft Internet Explorer
Edit View Favorites Tools Help
Search Favorites
http://www.marcorsyscom.usmc.mil/sites/ia/default.asp
Go

Marines
The Few. The Proud.

Integrated Logistics Capability
Making Change Happen – Logistically

Marine Corps Systems Command Logo.

Information Assurance

Home
Division Charter
Documents
Policy
Briefs
IAVA
Security Templates
References
Links
FAQs
Newsletter
MSTAR
Contact Us
IA Team Room
IA Registration

We're here for support and we live to serve.

To pause, move mouse over picture.

Mission:

To support the implementation of Information Assurance (IA) policies and practices for the Marine Corps in its effort to develop and field systems and applications that ensure confidentiality, authentication, non-repudiation, integrity, and availability of information systems and applications.

tp://www.marcorsyscom.usmc.mil/
Local intranet

INFORMATION ASSURANCE DIVISION
MARINE CORPS SYSTEMS COMMAND

Certification Requirements Review (CRR)

Initial meeting with the Information Assurance Team. The review is conducted in conjunction with the CA, Program Manager, and the User Representative to negotiate and agree upon the methodology for meeting all requirements , establishing security solutions, and managing the Information System security activities.

back

INFORMATION ASSURANCE DIVISION
MARINE CORPS SYSTEMS COMMAND

SYSTEM SECURITY AUTHORIZATION AGREEMENT

FOR THE

NEWLY DEVELOPED WARFIGHTER (NDW) SYSTEM

APRIL 2002

FOR OFFICIAL USE ONLY
(Refer to DoD 5200.1-R Appendix C, 2-200(5))

DISTRIBUTION STATEMENT D
Distribution authorized to the DoD and US DoD contractors only; Internal Documents; Apr 2002. Other requests for this document shall be referred to Commander (ATTN: C4ISR), Marine Corps Systems Command, Quantico, Virginia 22134-5010.

DESTRUCTION NOTICE
Non-record For Official Use Only (FOUO) documents may be destroyed by shredding or tearing into pieces and discarding the pieces in regular trash containers.

Prepared for:
Marine Corps Systems Command
Deputy Commander
Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
(C4ISR)
2033 Barnett Avenue
Quantico, Virginia 22134

Prepared by:
Northrop Grumman Information Technology
Marine Corps Support Team
2848 Jefferson Davis Highway
Suite 102
Stafford, VA 22554

FOR OFFICIAL USE ONLY

APPLICATION SECURITY PLAN

FOR THE

(System Name)

September 18, 2001

(Refer to DoDD 5200.1-R Appendix C)

DISTRIBUTION STATEMENT D
Distribution authorized to the DoD and US DoD contractors only; 2-200(5), Internal Documents; (Jul 2001). Other requests for this document shall be referred to Commander (ATTN: C4II), Marine Corps Systems Command, Quantico, Virginia 22134-5010.

DESTRUCTION NOTICE
Non-record For Official Use Only (FOUO) documents may be destroyed by shredding or tearing into pieces and discarding the pieces in regular trash containers.

Prepared for:
Marine Corps Systems Command
Deputy Commander
Command, Control, Communications, Computers, Intelligence & Integration
(C4II)
2033 Barnett Avenue
Quantico, Virginia 22134

FOR OFFICIAL USE ONLY

Rev 2.0
9/8/2001

back

System Security Authorization Agreement (SSAA)

The vehicle by which operational and security information is conveyed to the accreditation authorities. Template can be accessed by requesting access on the IA Website.

back

Application Security Plan (ASP)

A streamlined SSAA that may be appropriate for less complex applications to achieve DITSCAP Certification and Accreditation. Template is available on the IA Website.

back

Accreditation

The formal declaration by the Accreditor that an Automated Information System (AIS) is approved to operate in a particular security mode using a prescribed set of safeguards.

back

Parallel Processes

CCA **www.marcorsyscom.usmc.mil/ccaweb.nsf/index**

C4ISP
www.marcorsyscom.usmc.mil/sites/sei/C4ISPprocess.asp

IAVA **www.cert.mil**

IT-21 **https://infosec.navy.mil**

NSTISSP-11 **www.nstissc.gov/Assets/pdf/nstissp_11.pdf**

MCNOSC – ATC **https://www.noc.usmc.mil/**

SIPRNET CONNECTION
www.disa.mil/ciae/iapage.html

back

Clinger Cohen Act (CCA)

Law and policy requiring that we approach IT acquisition systematically, to include :

- **Addressing opportunities to improve processes before investing in the IT that supports them;**
- **Planning for IT as an Investment;**
- **Formulating an Information Assurance Strategy for the acquisition lifecycle.**

Confirmation of compliance with CCA has been defined by the Department of Defense as verifying compliance with eleven (11) key items

back

C4ISP

The C4I Support Plan provides a mechanism to identify and resolve C4ISR support shortfalls, and provide planned solutions at any given phase in a program's acquisition cycle.

www.marcorsyscom.usmc.mil/sites/sei/C4ISPprocess.asp

DOD 5000.2-R requires a C4ISP for all programs in all acquisition categories when they "connect in any way to communications and information infrastructure." Appendix 5 provides a mandatory format for C4ISPs, but also permits tailoring of the C4ISPs to match the complexity or other unique aspects of a program.

back

INFORMATION ASSURANCE DIVISION
MARINE CORPS SYSTEMS COMMAND

IAVA

Information Assurance Vulnerability Alerts are generated when a critical vulnerability has been identified that poses an immediate threat to DoD AIS systems and the need for corrective action is imperative.

www.cert.mil

back

INFORMATION ASSURANCE DIVISION
MARINE CORPS SYSTEMS COMMAND

IT-21

A NAVY accreditation process required for Automated Information Systems (AIS) which are utilized on a shipboard platform. SPAWAR is the process owner.

https://infosec.navy.mil

NSTISSP-11

The National Policy governing the acquisition of Information Assurance (IA) and IA-enabled Information Technology (IT) products. The January 2000 Policy is available at this link:

www.nstissc.gov/Assets/pdf/nstissp_11.pdf

MCNOSC – ATC

You must coordinate through the MCNOSC to receive an Authority to Connect from the MCEN DAA.

Phone: (703) 784-5300

SIPRNET CONNECTION

Information and Templates are available on the IA website as well as the DISA site given. Coordinate activities with MCNOSC at

DAA@noc.usmc.smil.mil

DODD 8500.1 Mission Assurance Category

- MAC is driving force behind the Operational Evaluation of IA
  - And the robustness of the IA evaluation
    - The more mission critical the system, the more in depth the evaluation!
- MAC I: “Vital” to mission effectiveness of deployed forces
  - Consequences of loss are unacceptable
  - Require the most stringent protection measures
- MAC II: “Important” to support deployed forces
  - Consequences of loss availability is difficult to deal with
  - Require additional safeguards beyond best practices
- MAC III: “Necessary” for the conduct of day-to-day business
  - Consequences of loss to deployed can be tolerated
  - Require protective measures commensurate with commercial best practices

Mission Assurance Category I

- DOD has three defined Mission Assurance Categories (MAC)
- Mission Assurance Category I (MAC I)
  - Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.
  - The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness.
  - MAC I systems require the most stringent protection measures.
- There is high risk to the mission if this system is lost or compromised

Mission Assurance Category II

- Mission Assurance Category II (MAC II)
  - Systems handling information that is important to the support of deployed and contingency forces.
  - The consequences of loss of integrity are unacceptable.
  - Loss of availability is difficult to deal with and can only be tolerated for a short time.
  - The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness.
  - MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.

There is medium risk to the mission if this system is lost or compromised

Mission Assurance Category III

- Mission Assurance Category III (MAC III)
  - Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term.
  - The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness.
  - The consequences could include the delay or degradation of services or commodities enabling routine activities.
  - MAC III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.
- There is low risk to the mission if this system is lost or compromised